Cyber security: Threats, Vulnerabilities and Countermeasures - A Perspective on the State of Affairs in Mauritius

Tikshnayah Nelliah Maistry, Nomesh Ramkurrun, Mageshwaree Cootignan and Pierre Clarel Catherine
School of Innovative Technologies and Engineering, University of Technology, Mauritius
La Tour Koenig, Pointe-aux-Sables, Republic of Mauritius
tmaistry@umail.utm.ac.mu, nramkurrun@umail.utm.ac.mu, mcootignan@umail.utm.ac.mu and ccatherine@umail.utm.ac.mu

ABSTRACT
Recent incident analysis from CERT-MU has found that there have been an increase in cybercrime activities including unauthorised access, electronic fraud, identity theft, denial of service, spamming and fake accounts. This paper describes the most common global vulnerabilities and threats and also provide an overview of countermeasures such as encryption, back-tracing and the use of common security standards and protocols such as ISO 127K. In addition, the security issues of emerging technologies such as IPv6, Internet of Things, and Cloud Computing are investigated. The system and infrastructure of the Mauritian Cybersecurity framework is also reviewed and recommendations are provided to build a strong and resilient cyber security framework in the country. This is particularly important given that Mauritius is embarking on the ambitious project of deploying smart cities with the integration of all these emerging technologies. Security must indeed be at the centre of all considerations in this endeavour.

KEYWORDS
Cyber security, network, attack, vulnerability, threats, Internet, IPv6, IoT

1 INTRODUCTION
In April 2011, around 100 million users were attacked worldwide through a distributed denial of service (DDoS) attack. The latter allowed the attackers to access the victims' PlayStation consoles and accounts. The company had to pay a £250,000 fine to the British regulators as it was unable to prevent its users' data such as account names, customer addresses and bank account numbers from leaking to the internet [1]. Stories such as that one are not uncommon in the current world, largely dominated by the pervasive use of ICT. This effect is accentuated with new technologies that makes it possible for electronic devices to now be connected to the "cyberspace". From mobile phones to video camera surveillance systems, from pacemakers to their remote monitoring systems, the "cyberspace" has become the main source of information and means of communication to most, if not all infrastructures. For this reason, cyber security has become a major priority of governments and corporations worldwide [2]. Cyber security enables the protection of assets such as building infrastructures, servers, desktop computers, information data and even lives. The objective is to protect data both at rest and during transmission [3].

However threats are becoming more aggressive with new attack methods and levels of sophistications. A correspondingly huge number of threatening issues were found on the web in 2014, and such trend is expected to continue this year and for years to come. New versions of malware and vulnerabilities suggest that the war to provide adequate level of security must be on a full-time basis [4].

The current work starts by providing an overview of common vulnerabilities and threats in section 2. Section 3 reviews the countermeasures available while section 4 provides an analysis of the growing sophistication of the cybersecurity landscape. Section 5 details some aspects of emerging technologies and the additional security concerns they raise. Sections 6 – 8 reviews the present security framework of Mauritius and

provides recommendations to enhance the latter. We finally conclude with section 10.

2 VULNERABILITIES & THREATS

A vulnerability is a hole or a weakness in an application and consists of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. A flaw can happen during coding, compilation or implementation of a software, also known as a bug, and allows an attacker to indirectly harm the stakeholders of the software. Stakeholders are entities that depend on the software as well as the software owner and users [5]. Most vulnerabilities, if not all, may allow a hacker to take advantage of the system by initiating an attack.

High security breaches can result in major drawbacks. In most cases, it is usually seen as the responsibility of IT managers who ignore IT systems vulnerabilities and bugs. IT security audit provides a way to reduce risks of attack, often by outsourcing the security of the system to a certified independent IT security professional or firm. The protection of the company's IT environment can then be managed properly without much input from IT managers. Penetration tests can be apply on a regular basis by performing security stress reverse test which look for and identify blind spots or the level of weaknesses and provide protection to those spots to avoid catastrophic security. Those tests are usually performed by the companies funded white hat hackers [6]. The most common software and web vulnerabilities are described in the next two subsections.

2.1 Most Common Software Vulnerabilities [7]

Some of the most common software vulnerabilities are:

a) *Injection*: Injections flaws, such as SQL (Structured Query Language), OS (Operating System) and LDAP (Lightweight Directory Access Protocol) injections happen when suspicious or infected data is unknowingly received by a user as part of request or order. The attacker's malicious data can fool the user into running unwanted requests or command codes which will enable unsanctioned data access to the attacker.

b) *Broken Authentication and Session Management*: Usually functions such as authentication and session management are wrongly implemented, providing a way for attackers to compromise credentials such as passwords and logins, keys, or session tokens or assuming another registered person's identity.

2.2 Most Recent Web Vulnerabilities & Attack

Some of the most recent web vulnerabilities and their corresponding attacks are next described:

a) "FREAK" [4]

A newly discovered vulnerability in the SSL (Secure Layer Security) and TLS (Transport Layer) cryptographic protocols could allow interception and decryption of communications of infected clients to and from servers. It facilitates man-in-the-middle (MITM) attacks against secure connections where there are unpatched or outdated version or OpenSSL this is a threat to the server which receive RSA_EXPORT cipher suites from the client with the outdated version. Further potential attacks can be launched to attack the website and steal password as well as private information.

b) "Heartbleed" [8]

Another vulnerability was recently found in the cryptographic software library of OpenSSL that may provide the attackers with access to session data such as private keys, passwords or credit card details inside a web's server memory during an encrypted session. This could provide open access to an entire encrypted data communication.

c) "ShellShock" or "Bash Bug"
ShellShock uses web servers via which attackers would use a Common Gateway Interface (CGI) which is commonly used for producing web content, to insert malware command code and infect operating system such as Linux distros, UNIX and even Mac OS X. [9].

d) Compromised Sites
Some web attack toolkits are designed to be used in the cloud, as software as a service (SaaS)
Web attack toolkits perform scans on the victims' computers, looking for vulnerable plug-ins in order to launch the most effective attack.
Attackers are also able to control how the exploits are administered such as enabling the attacks only if a cookie has been set by the initial compromised website thereby preserving the malicious code from the prying eyes of search engines and security researchers [10].

2.3 Type of Attacks

A cyber-attack is a digital attack to a website, computer systems (individual or networked computers) or it can be any connected electronic systems these days. The attacks may compromise the confidentiality, integrity or availability of the computer or information stored on it as well as the stability of a system. Cyber-attacks take many forms, including [11]:

a) Gaining, or attempting to gain, unauthorized access to a computer system or its data.
b) Denial of service (DoS) attacks by overloading and taking down of a whole web sites. There are multiple ways to execute a DoS attack. Some of the different forms of execution include:
    a. Teardrop - sending random size data packets over the network
    b. Buffer Overflow – the server is flooded with an excess of bogus data
    c. Smurf - tricking computers to reply to a fake request, causing much traffic

2.4 Targeted Attacks

Targeted attacks are designed to target and infiltrate specific organisations globally and steal data or cause some serious damage in any particular way required by the attacker. Some of these sophisticated attacks are designed for the purpose of cyber espionage.

2.4.1 Common Attack Groups and Platforms

Some notorious groups and platforms of attacks are presented:

a) Waterbug
Waterbug is a cyberespionage group that uses sophisticated malware such as Trojan. Wipbot and Trojan.Turla to systematically target government-related infrastructures in a range of countries [12]. One example of their attacks is Heartbleed which resulted in the loss of 4.5 million healthcare records [13] [14].

b) The Regin Platform
Regin is a cyber-attack platform that can monitor GSM networks as well as some other networks. The malware can attack by collecting key logs, making screen shots, stealing files from the system, and extracting emails from Microsoft email servers and information from network data flow. As GSM infrastructures are computer controlled, attackers can compromise the controller of the Base Station, which turn control the network and launch attacks via SMS and call interception or interruption. The Regin Platform targets specific groups such as telecom operators and research institutions [15].

c) Dragonfly
Dragonfly is an ongoing cyber espionage campaign, since 2011 that has the energy sector in Europe and US as target. Their goal is to steal information and is capable of sabotage along the way. The main targets are electricity infrastructure and generation, industrial equipment providers, and petroleum pipeline operators [16].

3 COUNTERMEASURES

Depending on the kind of attacks and their resources, defenders of an information system can use different variety of countermeasures [17]. These are next described.

3.1 Type of Countermeasures

a) Training

Employees of an organization should be aware of the kinds of attacks that is likely to occur in their organization and what they should do in such cases. Proper operating procedures should be adopted to protect key attack targets such as passwords. Several studies have indicated that education is more effective than any other countermeasure for protecting information systems since for most jobs, specific knowledge of information-systems security is not a prior requirement.

b) Legal Responses

Laws prohibit all mentioned attacks. But most attackers do not fear about getting caught, as it is they are usually very difficult to track and the laws prevailing cannot be easily applied, usually because of cross-border activities of the cyber criminals. Laws should however be effective against recidivist attackers.

c) Patches

It is important to fix flaws or bugs in software as soon as they are discovered, since flaws are typically exploited very soon after discovery and attacks are made within days. Manufacturers provide "patches", "security updates", or "service packs" to fix flaws, in the form of updated versions of software.

d) Backups

Since many attacks destroy data or programs, making copies ("backups") of digital information is essential to recover from attacks and to differentiate from tampered and genuine data. Backups should to be done for any critical information, and should to be stored some distance away from the systems which are vulnerable to attacks. A backup can be an entire duplicate computer system, server room or data centre.

e) Access Controls

Automated access controls are important for the cyberspace. Access controls for computers are generally managed by passwords that must be supplied to log on and use resources. Controls can be set for individuals or for groups of people, and they can apply separately to reading, writing, or execution of resources, or to the ability to extend those privileges to other users. Access controls for networks are enforced by "firewalls", dedicated computers on a local-area network that restrict traffic to and from the network according to simple rules on such features as origin and communications protocol. Unfortunately, access controls are vulnerable to many attacks mentioned above, and will not generally protect against attacks by insiders like technical staff.

f) Encryption

Encryption hides data in some form that cannot easily be read and a "key" must be supplied to decode it when required. Any attempts to modify encrypted data will result in undecipherability, so one can tell if encrypted messages or programs have been modified. Strong and virtually unbreakable methods of encryption have been developed with "public-key cryptography", and the software for it is available for free download from a number of Web sites. Encryption methods can also be used for "authentication" or to provide digital "signatures" on documents to prove who wrote them and when. Encryption has been touted as a solution to many security problems, but is usually overrated. Some of the recent encryption cipher includes AES and TKIP.

g) Intrusion Detection and Computer Forensics

Logging records the events on a computer system or network. This can generate enormous amounts of data. As such, intrusion-detection systems (IDSs) can be set up to check and record

the particular events that could indicate an attack, alerting system administrators when matters become serious. Signature checking is provided by standalone virus and worm application such as Norton Internet Security, Norton 360, McAfree, AVG, and Microsoft Security Essentials. Those anti-virus software will examine every file on a computer system to eliminate the "known" threats.

h) Intrusion Prevention Systems

Most of the methods mentioned so far just react to attacks. The alternative is an "active network defence system", which in its simpler forms is called also known as intrusion-prevention system. This includes simple things like turning off the Internet connection or logging out a user when they become sufficiently suspicious as judged by an intrusion-detection system. It can also include forms of limiting damage such as denying the user certain resources, downgrading their priority, or delaying them.

i) Backtracing

Backtracing is a form of active network defence that tries to find where an external attack is coming from so as to stop it more easily.

3.2 Security Standards and Protocols [18]

There are a number of international guidance undertaken by Integrated Computer Solutions (ICS) vendors to provide organisations and infrastructure, both in the private and public sectors locally with the best security services, standards and certifications possible. These are next depicted.

3.2.1 International Electrotechnical Commission (IEC) 62351

IEC is a standard developed for handling the security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection.

3.2.2 Institute of Electrical and Electronics Engineers (IEEE) 1686

Technical Standard for Security for Intelligent Electronic Devices.

3.2.3 Instrumentation, Systems, and Automation Society (ISA) 99 / IEC 62443

The ISA99 Committee establishes standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance.

3.2.4 International Organization for Standardization (ISO) 27K

The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.

3.2.5 NERC CIP

NERC CIP are standards that provide a cyber-security framework for the identification and protection of Critical Cyber Assets to support US, Canada and parts of Mexico's electrical grid operators.

3.2.6 NIST 800-53

Recommended Security Controls for Federal Information Systems and Organizations.

4 CYBER SECURITY CHALLENGES

A report from the World Economic Forum released in January 2014 examines the need for new approaches to increase resilience against cyber-attacks and suggests that the failure to effectively secure cyberspace could result in an aggregate impact of approximately US$3 trillion by 2020 [19].

Many of the challenges of cyber security are also challenges of privacy and data protection [20]. Cyber security will always need new and better systems with all the emerging technologies. The goal is to provide the best and strongest security available by keeping the data as private and secure as possible. Below are some emerging

challenges that need to be taken under consideration while amending standards:

4.1 Complexity of the Connected Network

As newer and bigger network are implemented for an increased connectivity of mobile devices and "always on" services, the cyberspace has become more complex and challenging to secure.

4.2 Growing Sophistication of Threats

With the increased load on devices, along came high end threats and professional hacking and cybercrime which make cybercrime activities much more difficult to counter and track. Now that the cyberspace has a much larger footprint across, in account of huge scale of information and data flow across, it has become clear that we are more exposed than ever without some "unbreakable security". The fact that companies almost never disclose security breaches for competitive and reputational purpose, it is even more difficult to work on and find solutions to those breaches on a global scale.

4.3 Threats moving to the Mobile Devices

The global population will be exceeded by the number of smart phones in use. Mobile devices may contain anything one need for their daily life routine from valuable personal data, office work. People usually carry their mobile devices with them almost all the time to keep in touch with their social world, access their bank accounts, surf the web, and monitor their health among many other activities. Organisations are always trying to reach to potential consumers on their everyday electronic devices. But this only give more possibility for new vulnerabilities for cyber threats. Malware can easily be distributed via app stores which may appear safe can also provide infected apps that can easily make their way to mobile devices [21]. Moreover, there is an increased risk of data being intercepted when connected to free public Wi-Fi [22]. "Tap-and-pay" functions can be compromised by malware and affecting local transactions [23]. An ICSPA study concluded that mobile malware is a key emerging threat in the cyberspace. Although it has been argued that cyber criminals are building better malware specifically designed for mobile devices, actual infection rates on devices are low for now since the distribution of malware to mobile devices has not yet been perfected. This can be expected to change in the near future [24]. Data protection will become more critical to mobile devices, and faced with this coming wave of threats to mobile devices, app developers, mobile industries and companies have a much greater responsibility in ensuring the safety of the mobile platforms.

4.4 The "Big Data" Paradox

"Big Data" can be characterised as a huge amount of data storage accumulated from both traditional sources, and progressively, new accumulation areas such as the web, sensors information, time, and locations extracted from social networks [25]. Results outcome from big data are often considered as answers to any issues that need solving [26]. But this brings up two different issues from cyber security point of view, firstly how secure is the data in Big Data context. Associations that choose to use the huge data available may present new potential security vulnerabilities and open many ways for malicious input [27]. As more networks and devices are connected, the risk of potential malware infecting devices increases. Big Data is definitely set to be one of the major breakthroughs of the recent years but it will certainly be the target of attackers out there. Hence the need for a proactive inclusion of security measures for Big Data.

5 EMERGING TECHNOLOGIES & SECURITY

Gartner predicted that the security technology and services market would reach $67.2 billion in 2013, up 8.7 percent from 61.8 billion in 2012. The market is expected to grow to more than $86 billion by 2016. The growth is partly due to interest in a new set of emerging security technologies and a return of more capable

defences that address mobile security, authentication weaknesses and threats to data in the cloud [28]. These technologies are next described along with some of the associated vulnerabilities as well as the countermeasures that can be undertaken.

5.1 IPv6

IPv6 has been introduced because IPv4 addresses were predicted to run out in the near future, which is the case with the rapidly increasing growth in IT and technology. This is where IPv6 solved the issues with its huge number of address space. But due to some security concerns many organisations have slacked off their transfer to IPv6 as the organisations realised that the security analysis and products for IPv6 might be inadequate in spite of the fact that the network infrastructure is ready to support IPv6 transport. IPv6 cannot be implemented without considering the security aspect. IPv6 security vulnerabilities currently exist and as the popularity of the IPv6 increases, the number of threats also is increasing.

5.1.1 Vulnerabilities Concerns with IPv6

a) Tracking the Identity of the User

For IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.

b) IPv6 Address Spoofing (MAC Address Spoofing)

Since IPv6 address depends on MAC address which in a sense the MAC address is a networked device's unique code name, used to identify devices from each other in a network. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. But with the right tools one might want to virtually change the MAC address of an NIC, also known as MAC Spoofing, for many reasons:

1. To get past MAC address filtering on a router.
2. Sniffing other connections on the network.
3. To keep their burned or blacklisted MAC address out of IDS and security logs.
4. To pull off a denial of service attack. Therefore, many attackers change their MAC addresses in different operating systems either manually or by specific tools. Unfortunately, this is privacy risk, because anyone who has your MAC address also has your IP address.

5.1.2 Multiple Addresses Vulnerability

IPv6 assigns multiple addresses to an interface which challenges the filtering rules in the firewalls and access control lists [29]. In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule sets. And such capabilities are not available.

5.1.3 Long Address Space

Port scanning is one of the most common techniques in use today. Port scanning allows "black-hats" to listen to specific services (ports) that could be associated to well-known vulnerabilities. In IPv6 networks, IPv6 subnets use 64 bits for allocating host addresses. Scanning such a large address space (264) is not absolutely impossible [30].

5.1.4 Fragmentation Security Vulnerability

Fragmentation is the process of dissecting an IP packet into smaller packets to be easily carried across a data network that cannot transmit large packets, fragmentation is never performed by the intermediary routers but by the end nodes themselves. So, only the end hosts are allowed to create and reassemble fragments. This process

may allow attackers to either hide their attacks or attack a node [31] [32].

Attackers can create fragments in such a way as to exploit weaknesses in the method an end host uses to defragment. Examples of this would be overlapping fragments, where there is an overlap in the offset and out-of-order fragments where the fragments' IDs do not match correctly with the data. Another type of fragment attack involves an attacker sending an incomplete set of fragments to force the receiving node to wait for the final fragment in the set. Fragmentation attacks also involve nested, where the IPv6 packet has multiple fragmentation headers. Fragmentation attacks are typically used by hackers with tools such as Whisker, Frag-router, Teardrop, and Bonk [33].

5.2 IPv6 Vulnerabilities Control

There are a number of steps to be taken so as to minimise the threats to IPv6. Below are a few guideline that needs to be taken under consideration:

1. Use standard, non-obvious static addresses for critical systems,
2. Ensure adequate filtering capabilities for IPv6,
3. Filter internal-use IPv6 addresses at border routers,
4. Block all IPv6 traffic on IPv4-only networks,
5. Filter unnecessary services at the firewall,
6. Develop a granular ICMPv6 filtering policy and filter all unnecessary ICMP message types,
7. Maintain host and application security with a consistent security policy for both IPv4 and IPv6,
8. Use IPsec to authenticate and provide confidentiality to assets,
9. Document the procedures for last-hop trace back and,
10. Pay close attention to the security aspects of transition mechanisms.

5.3 IPSec

IPSec, is a framework of open standards from Internet Engineering Task Force (IETF) that provides secure communications in a network by providing cryptographically-based security for IPv4 and IPv6. It offers different security administrations at the IP layer and in this way, offers security to the network layer and higher layers of the stack. The security administrations include: instance, access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality [34].

5.4 Cloud Computing

Cloud computing enables application software to be operated utilizing internet-enabled devices. Clouds can be categorized as public, private, and hybrid. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, homogeneous to a utility such as the electricity grid over a network. At the substructure of cloud computing is the broader concept of converged infrastructure and apportion accommodations. Cloud computing, or in simpler shorthand just "the cloud", additionally works on maximizing the efficacy of the shared resources. Cloud resources are conventionally not only shared by multiple users but are additionally dynamically reallocated per demand. This can work for allocating resources to users [35].

5.4.1 Security of the Cloud

Cloud computing security or simply cloud security is a developing sub-area of Computer security and network security. It refers to a wide set of policies, technologies, and controls conveyed to secure information, applications, and the related framework of cloud computing. Cloud security architecture is powerful only if the right protective usage are set up. A proficient cloud security infrastructure will need to address the issues that will emerge with security administration and security controls. These

controls are set up to protect any shortcomings in the framework and decrease the impact of an attack [36].

5.5 IoT [37]

The vision of the internet of things (IoT) is to manage objects around us with their own unique identifiers such as IP addresses and MAC addresses. IoT will consist of billions of devices that can sense, communicate and take actions. The rise of IPv6 also contributes to the uptake of the Internet of Things [38]. Fundamentally IoT will give the capacity of transferring information to more than a network without the need of human-to-human or human-to-PC association, and will rely mostly on Machine to Machine (M2M) communications. The definite size of the Internet of Things is difficult to gauge, as its development is gigantic and will very soon surpass whatever remains of the Internet in size (number of nodes) and will keep developing at a fast rate, maybe even in trillions of devices. The best development potential will probably come from embedded, low-power, wireless devices and systems that were not previously IP-enabled, opening up the era of the Wireless Embedded Internet.

6 OVERVIEW OF CYBER SECURITY INFRASTRUCTURE IN MAURITIUS

Mauritius is one of the few African countries that has legislations, laws and infrastructures that govern cyber security and help against related cybercrime activities. Mauritius along with many other countries have been working with ITU, and in collaboration with key partners, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), to facilitate the development of cybersecurity capabilities, including the establishment of national CIRTs [40]. The security system in Mauritius is quite robust and redundant but there still some issues to be taken under considerations. In this section, the security framework of Mauritius is reviewed.

6.1 ICT Laws against Cyber Crime

There are a couple of ICT Laws that help govern the Mauritian Cyberspace [41];

6.1.1 Computer Misuse and Cyber-Crime Act 2003

The Act was enacted to provide for repression of criminal activities perpetrated through computer systems and to help reduce cybercrimes impact on the society and discourage to give a strong signal to would-be perpetrators. Cyber criminals may face severe penalties and fine for examples if found guilty for unauthorised access to restricted data and with intent to commit offences.

6.1.2 Data Protection Act 2004

The goal of this Bill is to accommodate the security of the protection privileges of people in perspective of the improvements in the procedures used to capture, transmit, and control, record or store information identifying with people. Protection laws refers to the privileges of people or associations to limit the utilization of information

6.1.3 The Information and Communication Technologies Act 2001

It provides the appropriate legal framework to facilitate electronic transactions and communications and give a new orientation to the traditional way of doing business by fostering the conduct of transactions by electronic means. It also provides for the legal recognition and regulation of electronic records, electronic signatures and their security. This allows devices to authenticate authorised access only.

6.2 Information Security Management System (ISMS) [42]

The ISMS under the Ministry of Technology, Communication and Innovation (MTCI) is a set of policies concerned with information security management or IT related risks. It is a system designed to establish, implement, operate,

monitor, review, maintain, and improve information security. ISMS can be implemented as a specific information system that deals with a particular business area, or it can be implemented as an all-encompassing system involving the whole organization. The IT Security Unit facilitates the implementation of ISMS in Ministries and Departments by providing training to officers in information risk management, providing advice to their Information Security Forums, reviewing and auditing the ISMSs.

6.2.1 Standards provided by the Mauritius Standards Bureau.

- MS ISO/IEC 27001 - The Information Security Management System

This standard addresses the topic of information security management and provides a framework to initiate, implement, maintain and manage information security within an organisation.

- MS ISO/IEC 27002 - Code of Practice for Information Security Management

This is a standard code of practice which contains guidelines to be followed to set up and implement the ISMS. It can be regarded as a comprehensive catalogue of good security things to do.

6.2.2 ISMS Implementations

There are around 10 sites of the Government that are presently implementing their ISMSs. Two of which have already been certified at the national level as of March, 2015 [43]:

- Cane Planters and Millers Arbitration and Control Board

The Control and Arbitration Department has established and applied an Information Security Management System to protection the information it receives, deal with, saves and communicates while supplying arbitration and control services to Cane Planters and Millers.

- Passport and Immigration Office (PIO)

The passport and immigration office has established and applied an information security management system to protect the information it receives, deals with, or communicates while supplying its services for the issuance of passports and travel documents, immigration activities at the head office and offices at SSR International Airport and the Aurelie Perrine Passenger Terminal.

6.3 Central Informatics Bureau

The Central Informatics Bureau operates under the aegis of the MTCI. Its main function is to promote e-Governance through the provision of project management, consultancy and advisory services to Ministries and Departments for the successful implementation of e-government projects and on ICT matters.

6.4 National Computer Board (NCB)

The NCB comprises of many subsections and teams that work to help bring down cybercrime activities and bring awareness to the public. Some of those subsections are the GOC and CERT-MU.

6.4.1 Mauritius National Computer Security Incident Response Team (CERT-MU)

CERT-MU was set up by National Computer Board in May 2008 to handle and coordinate information security issues at the National level, as well as the managing of Information Security risks, such as Information Security breaches and incidents. CERT-MU Services includes [44]:

- Incident Response and Coordination
- Vulnerability Scanning and Assessment
- Assistance in the Implementation of ISO27001
- Information Security Audits
- Information Security Awareness
- Technology Workshops
- Capacity Building
- Presentations
- Issuance of Security Alerts
- Advisories & Vulnerability Notes
- Virus Alerts
- Information Security News

Basically the main objective is to provide to provide information and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur.
There some entities such as information infrastructure providers, system administrators both in the public and private sectors and the common public that benefit from security threats warning and as well as guidance on how handle those security risks [45].

6.4.2 Incident Statistics Reported

Incident statistics reports from CERT-MU shows an increased in certain cybercrime activities in Mauritius. While some activities were controlled, some others emerged. The following activities were increased from 2013 to 2014: unauthorised access by 3%, electronic fraud by 1%, identity theft by 3%, DoS attack by 1%, spamming by 2%, website defacement by 1%, offensive video by 1%, fake account by 22% [46] [44].

6.4.3 Cyber Security Mauritius Website

The website is under CERT-MU and helps instruct and improve the attention to the overall population on the technological and social issues confronting web clients, especially on the risks online. The Cyber Security Mauritius expects to give data to distinctive focused on gatherings, such as children, parents, home users and organisations.

6.4.4 The Government Online Centre

The Government online centre is the gateway to access applications online through one of its sub-portals, the Citizen Portal. 66 e-Services are online for the Citizen of Mauritius to interact with the Government anytime, anywhere and in real time. Operational since May 2005, the GOC is overseen by NCB and situated in the Ebene Cyber Tower. GOC takes a proactive, complete approach by giving its clients the business' most intense security devices and methods, designed, assembled and kept up particularly for big business class application hosting. From secure server manufactures and intrusion protection frameworks to a physically secure data centre and observed system, the GOC takes a multi-layered way to deal with keeping all application hosting operations dependable and secure.

7 IMPROVING SYSTEMS & SECURITY IN MAURITIUS CYBERSPACE

As new technologies and threats emerge, the need for system security upgrades are needed to counter the newer threats and continue protect those systems.

7.1 R&D (Research & Development)

Mauritius rely solely on other international cybersecurity organisation and research. Like other leadings countries, Mauritius does not have any R&D unit when it comes to fighting new cyber threats. As new technologies such as Smart Cities, IPv6, Cloud and IoT are emerging in Mauritius, a new infrastructure should be dedicated to the whole purpose of finding new methods of fighting cybercrime activities in collaboration with other stakeholders in Mauritius. This R&D unit should be specific for the system requirements of Mauritius.

7.2 Improved Governance Structure [48]

A new governance structure was proposed by the Ministry of ICT to ensure security development. The goal of the new structure is set in the National Strategy for Cybersecurity, 2014-2019, (see figure 1):

- Securing Mauritian Cyberspace

The aim is to set a cyber-defence strategy that prevents cyber-attacks by improving capabilities, defining roles and developing

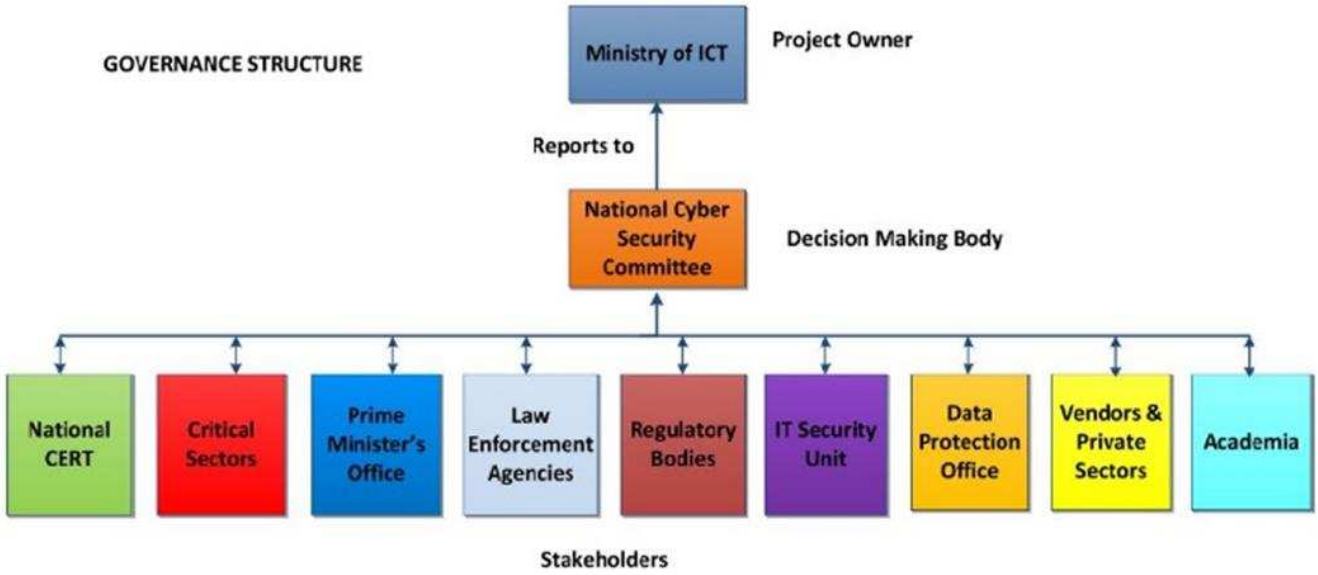

Figure 1: Governance Structure proposed by the National Computer Board

necessary responses for the public and private sector.

By creating a sense of awareness of the vulnerabilities, threats and the ability to react faster to prevent intrusions in our cyberspace. More laws should be enforced to investigate and prosecute cybercrimes.

- Enhancing resilience to Cyber Attacks

Efforts should be intensified to protect our critical network infrastructure in order to improve our resilience to cyber-attacks and to support various national projects and to maintain economic stability. Disruptions in the critical infrastructure can affect negatively the ability of a nation to perform effectively. The objective is to identify any disruptions in the cyberspace and to try to minimize their effects.

- Developing a collaboration between various authorities

There should be an active collaboration between the stakeholders whose aim is to achieve a nation free from cyber threats. Critical IT infrastructure and systems will be identified and will be protected. Cyber vulnerabilities assessments will be carried out and the Cyber Defence will be advanced.

- Improving Cyber Expertise

Cyber Security professionals and capacity building to deter and defend cyber threats should be encouraged. In this modern society, the level of competence of the professionals should be raised and to do so, a cadre of skilled cyber professionals should be promoted.

7.3 Encourage Active Monitoring System

Rather than relying only on passive security techniques or reactive defensive measures, organisations in Mauritius can better benefit from an active autonomous defence system that will automatically detect and eliminate the threats. Proactive procedures that enable the framework to identify attacks at an opportune time, and quickly react to neutralize the danger is becoming increasingly important.

7.4 Centralisation of Cybersecurity Infrastructure

The centralisation of the Government databases at a single location would represent an important step in the right direction. Currently, many of

these databases contain fragmented information. As such, centralising these information systems will reduce confusion and provide only the most updated version of the information required. In addition, the security aspect would be greatly simplified. Such structure however does not preclude the building of secondary sites that replicates the data for back-up and recovery purposes.

8 CONCLUSION

Computer security endeavours to guarantee the secrecy, trustworthiness, and accessibility of computing systems and their segments. Three essential parts of a computing systems are liable to attacks: hardware, software, and data. These three, and the communications among them, are prone to computer security vulnerabilities. As Mauritius is interested in making the Information Technology Sector its main pillar of the economy by introducing Smart Cities, Internet of Things and Cloud computing among other innovative technologies, the need for better cyber security infrastructures is becoming increasingly important. Although cyber-attacks are generally the work of individual hackers, challenge gatherings, or criminals looking for unlawful monetary benefit, some likewise represent a risk to national security. To meet the security challenges of tomorrow, we must enhance our capacity to identify, research, and react to cyber-attacks today. For the case of Mauritius, the establishment of a National Cyber Security Committee is considered crucial. That committee would then take up the challenge of coping with the changing technology landscape and all the security issues this will involve.

9 REFERENCES

[1] R. Williams, "The biggest ever cyber attacks and security breaches," Telegraph Media Group Limited, 22 May 2014. [Online]. Available: http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggest-ever-cyber-attacks-and-security-breaches.html. [Accessed May 2015].

[2] R. Deibert, "Distributed Security as Cyber Strategy:Outlining a Comprehensive Approach for Canada in Cyberspace," 2012.

[3] S. Musa, "The Evolllution," 2013. [Online]. Available: http://www.evolllution.com/opinions/cybersecurity-understanding-online-threat/.

[4] S. R. T. Symantec, "FREAK vulnerability can leave encrypted communications open to attack | Symantec Connect," Symantec Corporation, 4 March 2015. [Online]. Available: http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack. [Accessed May 2015].

[5] O. W. A. S. P. OWASP, "Open Web Application Security Project," 5 April 2014. [Online]. Available: https://www.owasp.org/index.php/Category:Vulnerability.

[6] S. Bavisi, Computer and Information Security Handbook, Morgan Kaufmann Publications, Elsevier Inc, 2009.

[7] O. W. A. S. P. (OWASP), "OWASP," Open Web Application Security Project (OWASP), 2013. [Online]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10.

[8] D. O'Brien, "Heartbleed Bug Poses Serious Threat to Unpacthed Servers | Symantec Connect," Symantec Corporation, 4 April 2014. [Online]. Available: http://www.symantec.com/connect/blogs/heartbleed-bug-poses-serious-threat-unpatched-servers. [Accessed 2015].

[9] T. Symantec Security Response, "ShellShock: All you need to know about the Bash Bug vulnerability | Symantec Connect," Symantec Corporation, 25 September 2014. [Online]. Available: http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability. [Accessed May 2015].

[10] C. Symantec, "Internet Security Threat Report, Volume 20," Symantec Corporation, 2015.

[11] B. M. a. R. R. H. K. L. Vince Farhat, "Cyber Attacks:Prevention and Proactive Responses," Practical Law Publishing Limited and Practical Law Company, Inc., 2011.

[12] C. Symantec, "Internet Security Threat Report, Volume 20," 2015.

[13] N. BBC, "BBC News - US hospital hack 'exploited Heartbleed flaw'," BBC News -, 20

August 2014. [Online]. Available: http://www.bbc.com/news/technology-28867113. [Accessed May 2015].

[14] S. R. T. Symantec, "Torjan.Turla | Symantec," Symantec Corporation, 2014. [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2014-011316-1921-99.

[15] L. Kaspersky, "The Regin Platform | What is Regin? | Virus Definition," 2015.

[16] A. Forzieri, "Secure and Protect your Critical Infrastructure," in *Computer Security Day 2014* , 2014.

[17] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, vol. 4, 2007.

[18] A. Forzieri, "Secure and Protect your Critical Infrastructure," in *Computer Security Day 2014*, Mauriitius, 2014.

[19] McKinsey, "Risk and Responsibility in a Hyperconnected World," World Economic Forum, 2014.

[20] O. o. t. P. Commissioner, "Privacy and Cyber Security," Office of the Privacy Commissioner of Canada, 2014.

[21] A. S. B. a. M. Lockheed Martin, "International Cyber Security Protection Alliance," 2013.

[22] I. C. S. P. Alliance, "Study of the Impact of Cyber Crime on Businesses in Canada," 2013.

[23] M. Labs, "McAfee 2013 Threats Predictions Report," 2013.

[24] A. Gonsalves, "Windows malware finds its way to Android | Computerworld," 16 August 2013. [Online]. Available: blogs.computerworld.com/mobile-security/22662/windows-malware-finds-its-way-android?source=CTWNLE_nlt_security_2013-08-19.. [Accessed May 2015].

[25] C. f. I. P. Leadership, ""Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance,"," 2013.

[26] E. Schmidt and D. Wagner, Interviewees, *Why Data Analytics Is the Future of Everything.* [Interview]. 21 November 2013.

[27] P. Wood, "How to tackle big data from a security point of view," 5 September 2013. [Online]. Available: http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view. [Accessed May 2015].

[28] R. Westervelt, "10 Emerging Security Technologies Gaining Interest, Adoption," CRN, 17 June 2013. [Online]. Available: http://www.crn.com/slide-shows/security/240156647/10-emerging-security-technologies-gaining-interest-adoption.htm. [Accessed May 2015].

[29] A. S. A. Choudhary, "Securing IPv6 Network Infrastructure: A New Security Model," in *IEEE Conference*, USA, 2010.

[30] P. Risztics, "Will IPv6 Bring Better Security?," in *30th Euromicro Conference*, 2004.

[31] D. G. J. B. a. Y. P. K. Merike, "IPv6 Security Technology North," 2006.

[32] M. H. Warfield, "Security Implications of IPv6 Whitepaper," 2003.

[33] S. Hogg and E. Vyncke, "IPv6 Security," Cisco Press, USA, 2009.

[34] K. Das, "IPv6.COM - IPv6 and IPSec - Securing the Next Generation Internet," IPv6.com, 2008. [Online]. Available: http://ipv6.com/articles/security/IPsec.htm. [Accessed May 2015].

[35] H. Qusay, ""Demystifying Cloud Computing"," *The Journal of Defense Software Engineering*, pp. 16-21, 2011.

[36] a. R. D. V. Krutz Ronald L., ""Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing," Indianapolis, 2010.

[37] S. P. Pawar, "Smart City with Internet of Things (Sensor networks) and Big Dat," 2015. [Online]. Available: http://www.academia.edu/5276488/Smart_City_with_Internet_of_Things_Sensor_networks_and_Big_Data. [Accessed 2015].

[38] *Internet of Things.* [Film]. USA: TEDxCIT, 2014.

[39] D. Maughan, "DHS S&T Showcase New Cybersecurity Technologies | Homeland Security," DHS, 23 August 2013. [Online]. Available: http://www.dhs.gov/blog/2013/08/23/dhs-st-showcase-new-cybersecurity-technologies. [Accessed May 2015].

[40] ITU, "ITU Regional Cybersecurity Forum for Africa and Arab States," ITU, Tunis, Tunisia, 2009.

[41] I. a. C. T. A. o. Mauritius, "ICT Authority | ICT Laws," ICTA, 11 May 2015. [Online]. Available: https://www.icta.mu/laws/ict_laws.htm. [Accessed May 2015].

[42] .. Mauritius Standards Bureau, "Mauritius Standards Bureau - Information Security Management System," MSB, [Online]. Available:

http://msb.intnet.mu/English/AboutUs/Pages/Structure.aspx. [Accessed 2015].

[43] .. Mauritius Standards Bureau, "Mauritius Standards Bureau - Certification Schemes - Information Management System," 2015. [Online]. Available: http://msb.intnet.mu/English/Certification%20Schemes/Pages/Information-Security-Management.aspx. [Accessed June 2015].

[44] R. Sachindra, "The Current Legal Framework on Cybercrime in Mauritius," CERT-MU, 2014.

[45] MTCI, "Mauritian National Computer Security Incident Response Team > About CERT-MU > Charter & Mission," 2015. [Online]. Available: http://cert-mu.govmu.org/English/About_CERT-MU/Pages/Charter--Mission.aspx. [Accessed May 2015].

[46] K. Usmani, "An Enhanced Framework For Incident Handling," CERT-MU, Port Louis, 2014.

[47] NCB, "National Computer Board | Government Onlince Centre," 2015. [Online]. Available: http://www.ncb.mu/English/EPowering%20Public/Pages/Government-Online-Centre.aspx. [Accessed May 2015].

[48] MTCI, "National Cyber Security Strategy," Port Louis, 2014-2019.

[49] ICTA, "The ICT Sector in Mauritius," ICTA, Port Louis, 2004.

[50] Y. E. Gelogo, R. D. Caytiles and B. Park, "Threats and Security Analysis for Enhanced," *International Journal of Control and Automation*, vol. 4, no. 4, pp. 179-184, 2011.

[51] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," 2007.

[52] N. M. CERT-MU, "Cybersecurity Mauritius Home," NCB, [Online]. Available: http://cybersecurity.ncb.mu/English/Pages/default.aspx. [Accessed May 2015].

[53] MTCI, "Ministry of Technology, Communication and Innovation - ISMS Implementation," 2015. [Online]. Available: http://mtci.govmu.org/English/Pages/IT%20Security/ISMS-Implementation.aspx. [Accessed May 2015].